CLEAN VERSION OF AMENDMENTS

IN THE SPECIFICATION

Please enter the following Substitute Specification and Abstract, in replacement of the originally filed specification and Abstract:

SUBSTITUTE SPECIFICATION

TITLE

COPY PROTECTION SYSTEM FOR PORTABLE STORAGE MEDIA

CLAIM FOR PRIORITY

[0001] This application makes reference to, incorporates the same herein, and claims all rights accruing thereto under 35 U.S.C. §119 through our patent applications entitled *The Digital Content Encryption Apparatus And Method Thereof* earlier filed on the 24th day of September 1998 in the Korean Industrial Property Office and there duly assigned Serial Nos. 1998/39808 and 1998/39809.

FIELD OF THE INVENTION

[0002] The present invention is generally related to encryption processes and apparatus, and, more particularly, to secure and robust processes and apparatus for the generation and use of keys in the transmission and replay of digital information for licensed Secure Digital Music Initiative (SDMI) compliant modules such as personal computers and SDMI compliant portable devices in conjunction with Internet service content provider and a certificate authority.

BACKGROUND ART

[0003] Recently, with the flood of information provided by various media such as broadcasting and press, an atmosphere has been created by the information providers who are interested in providing integrated information that covers all of the media. Other users want to selectively receive a specific item of digital information from the entire spectrum of information available from a particular information provider (IP). Accordingly, a digital content transmission system has been formed by the information providers who convert various types of information into a digital form and store this digital information, and the users who subscribe to this digital information system from the information provider via the network. Digital information transmission systems endow an application program with easy downloadability of the digital content. The user can get all the information desired by using this application program to access the digital information system through the network.

[0004] The digital information may be provided to the user either for pay or for free. In case of paid digital information, the server who provides the digital information via the transmission system sets the service fee. The service server charges the user according to the quantity of information used when the digital information is downloaded to the user. MPEG software protocol for example, compresses audio files to a fraction of their original size, but has little perceptible effect upon the quality of the audio sound. MPEG software protocol is now widely used by Internet sites offering digitalized music, and is reported to be commonly used to offer digitalized versions of recorded music without the consent of the musicians. When a user is connected to a server that provides digital information commercially via a network, a few of the users may be able to inadvertently or illegally copy the digital information, a practice that, as was recently noted by Interdeposit and the French Agency for the Protection of Programs, a member of the European Association of Authors and Information Technology Professional, in the *Patent, Trademark & Copyright Journal*, volume 57, No. 1416, page 385 (11 March 1999), would be economically damaging to both the musicians and to the server who is running the digital information transmission system. Currently, the server, as well as the musicians, can do little more than seek redress by undertaking civil and criminal action in an effort to control the possibility of unlicensed reception of digital information. We have noticed that there is a need for a technique to preserve transmission security of revenue bearing information while restricting access to the information by unauthorized entities and preventing unauthorized users from using any of the information that they may be able to illicitly obtain from the information provider by restricting the ability of the unauthorized users to decrypting whatever information they manage to obtain via the system.

[0005] Also, it is difficult to prevent the illegal copy of the supplied digital contents or the codec recorded on the portable medium if the portable medium is copied after the digital content has been supplied to a user and recorded on the portable medium.

[0006] In particular, the MP3 which is the audio data of the above digital contents is downloaded to the first content output unit as well as the second content output unit such as an MP3 player and then reproduced. In the meantime, the MP3 is downloaded to a content storage unit such as a smartmedia card built in the first content output unit, and the MP3 downloaded in the content storage unit is reproduced through the second content output unit.

[0007] However, as stated above, there is a drawback in that the digital data downloaded to the first and second content output units and the content storage unit are easily copied to be illegally distributed

SUMMARY OF THE INVENTION

[0008] It is therefore, one object of the present invention to provide improvements in cryptographic processes and apparatus.

[0009] It is another object to provide a secure and robust digital encryption process and apparatus.

[0010] It is yet another object to provide digital encryption processes and apparatus endowing a system with secure and robust copy protection for a licensed secure digital music initiative compliant module such as personal computers and portable devices such as disk and DVD players in conjunction with Internet service provider and a certificate authority.

[0011] It is still another object to provide digital encryption processes and apparatus able to encrypt and transmit digital information received from a transmission system, by the use of multiple cryptographic keys.

[0012] It is still yet another object to provide digital encryption processes and apparatus for generating and using multiple cryptographic keys during the transmission of digital information to a user.

[0013] It is a further object to provide digital encryption processes and apparatus that employ user information in the generation and use of multiple cryptographic keys during the transmission of digital information to the user.

[0014] It is a yet further object to provide digital encryption processes and apparatus able to encrypt and transmit digital information obtained from a transmission system by using multiple cryptographic keys, and to decrypt and play the digital information at the terminal of the user by using a plurality of keys, one of which is common to the multiple keys.

[0015] It is a still further object to provide digital encryption processes and apparatus able to encrypt and transmit digital information obtained from a transmission system by using key information, a user's key, and a temporary validation key, and to decrypt and play the digital information at the terminal of the user by using the key information and user authorization information.

[0016] It is still yet a further object to provide encryption, transmission and reception protocols enabling encryption, transmission and decryption of digital information received from a transmission system.

[0017] It is an additional object to provide encryption, transmission and reception protocols enabling encryption and transmission of digital information received from a transmission system by using multiple keys to encrypt the digital information, and decryption and replay of the digital information at the terminal of the user by using a plurality of keys, one of which is common to the multiple keys.

[0018] It is still yet a further object to provide encryption, transmission and reception protocols enabling encryption and transmission of digital information received from a transmission system, by using key information, a user's key, and a temporary validation key, and decryption and replay of the digital information at the terminal of the user by using the key information and user authorization information.

[0019] It is also an object to provide a more secure cryptograph and process for transmitting information to a terminal of a user who has requested the information.

[0020] It is also a further object to provide a cryptograph and process that reliably restricts the ability of a registered subscriber who has validly obtained information from an information provider, to deliver that information to another entity in a readily usable form.

[0021] These and other objects may be attained with an encryption process and apparatus that provides a secure and robust copy protection system for a licensed secure digital music initiative compliant module such as personal computers and portable devices, in conjunction with Internet service providers and certificate authorities, by responding to a user's request for transmission of items of digital information to the user's terminal unit, by providing copy protection during downloading and during uploading of the digital contents. In order to prevent the digital contents from being copied illegally, a plurality of keys is generated and held by both the user and the digital content provider, and a secret channel is formed between both the user and the digital content provider. The header of the encrypted digital content is encrypted by using a physical address of a sector of a licensed SDMI compliant module such as a portable computer or a portable media device in order to prevent the digital content from being copied illegally after the digital content is recorded in the portable media.

[0022] The present invention includes a certificate authority, an information provider, a first content output unit, a second content output unit, and a manufacturer of the second output units.

[0023] The certificate authority generates, encrypts, and outputs a first authentication qualification key and a first authentication qualification key data, and generates a manufacturing key and manufacturing key information in response to a registration request signal from the manufacturer, The certificate authority forms a first table and a second table. The first table has a manufacturer key, a manufacturer key data, and information of the manufacturer key, and the second table has a token, a token information encrypted by the manufacturer key, the identification of a portable device or terminal.

[0024] The manufacturer of the second output units such portable devices sends a registration request signal to the certificate authority and receives the manufacturing key and manufacturing key data.

[0025] The internet service provider transmits the registration request signal to the certificate authority, stores the first authentication qualification key and the first authentication qualification key data inputted from the certificate authority in order to be authorized to supply the encrypted digital contents, and generates a second authentication qualification key and a second authentication qualification key data. The internet service provider outputs the second registration request signal to the certificate authority,

[0026] The first content output unit such as a personal computer outputs the registration request signal to the internet service provider in order to receive the digital contents, stores the second authentication qualification key and the second authentication qualification key data, outputs the manufacturer key data to the internet service provider, encodes and outputs the manufacturer key detected from the second table in response to the manufacturer key data, and receives a public key, public key information and digital contents

[0027] The second content output unit such as a portable device outputs the first registration request signal to the certificate authority and stores the manufacturer key and the manufacturer key data inputted from the certificate authority.

[0028] In addition or alternatively, the present invention may use a physical address of a bad sector formed in the portable recordable medium during the manufacturing process, encrypts a header of the encrypted digital contents stored in the portable recordable medium, and records the encrypted header on the physical address of the bad sector of the portable recordable medium for preventing an illegal copy of the downloaded digital contents through a terminal after the digital contents have been downloaded.

BRIEF DESCRIPTION OF THE DRAWINGS

[0029] A more complete appreciation of this invention, and many of the attendant advantages thereof, will be readily apparent as the same becomes better understood by reference to the following detailed description when considered in conjunction with the accompanying drawings in which like reference symbols indicate the same or similar components, wherein:

[0030] Fig. 1 is a block diagram illustrating the overall architecture of an implementation of the principles of the present invention;

[0031] Fig. 2 is a block diagram illustrating a registration by an original equipment manufacture of a portable device with a certificate authority;

[0032] Fig. 3 is a block diagram showing the registration of an Internet service provider's registration with a certificate authority;

[0033] Fig. 4 is a block diagram showing the registration of a personal computer and a portable device with an Internet service provider;

[0034] Fig. 5 is a block diagram showing usage rules governing a database of a right management system;

[0035] Fig. 6 is an exemplified format;

[0036] Fig. 7 is a block diagram showing the basic architecture for various inputs;

[0037] Fig. 8 is a block diagram showing control of outsource import; and

[0038] Fig. 9 is a block diagram showing a copy protection system for portable media.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0039] Hereinafter, a preferred embodiment of the present invention will be described in detail with reference to the accompanying drawings.

[0040] For the removal of some ambiguities, in this section, we define some terminologies and list up some abbreviated words for a simple description.

[0041] First, we have to distinguish the two words, "Portability" and "Transferability" of a content.

[0042] Portability means that a content in a portable media (PM) can be played in any portable device (PD). Transferability means that "portability" plus "upload of a content is allowed from a portable medium to even a LCM."

[0043] The digital contents which are used in the present invention mean all data including audio, video data, as well as character data such as song words, movie caption, and the like to be provided through internet.

[0044] Herein after we use the following abbreviated words.

[0045] CA stands for a certificate authority (e.g., secure digital music initiative (SDMI), or other trust third party). LCM stands for a licensed SDMI Compliant Module. PD stands for an SDMI compliant portable device. PDFM stands for a portable device functional module. ISP stands for an Internet Service Provider (including content providers via the Internet). PM stands for a portable media (SDMl compliant storage media).

[0046] Furthermore, here are presented some notations to be used in the following sections. Even though they are some intricate, we are sure that they would help the readers clearly understand the concrete method we intend. They are relevant to the algorithmic functional modules.

(AIF) Algorithm Identifying Field;

(API) Applied Program Interface;

(CA) Certificate Authority;

(CCS) Copy Control Status;

(CDF) Content Description Field;

(CEK) Content Encryption Key;

($Cert_{CA}$ ($PubKey_A$)) Certificate (Data) for $PubKey_A$ issued by CA;

(CHI) Copyright Holder Information Field;

(CK_{PD-LCM}) a secure (secrete) channel key which is set up between PD and LCM;

(CTC) Copyright, Transfer, Check-in/Check-out;

(DEC(*key,*C)) Symmetric key decryption of a ciphertext C by utilizing a secret key, *key*;

(ECC) Elliptic Curve based Cryptosystem;

(EC_DEC) Elliptic Curve Decryption of a ciphertext (encrypted text) by utilizing a private key;

(EC_DH(*A,B*)) a random secret value (key) shared between A and B by Elliptic Curve based Diffie-Hellman Key Exchanging Protocol;

(EC_DH(ISP,LCM) random secret value (key) shared between ISP and LCM by Elliptic Curve (Cryptosystem) based Diffie-Hellman Key Exchanging Protocol;

(EC-ENC) Elliptic Curve-based Encryption of a content by utilizing a public key;

(EC_ENC(*key, C*)) Elliptic Curve based Encryption of a ciphertext (encrypted text) *C* by utilizing a private key, *key*;

(ENC) Symmetric Key Encryption of a content by utilizing a secret key;

(ENC(*key, C*) Symmetric Key Encryption of a content C by utilizing a secrete key, *key*;

(ICL) Import Control Layer;

(ID_A) Identifier of A;

(IP) Information Provider;

(ISP) Internet Service Provider including Content Provider via the network;

(LCM) Licensed SDMI Compliant Module;

(MKIT) Manufacturer Key Information Table;

(MK_{PD}) Manufacturer Key within a portable device;

(PCS) Playback Control Status;

(PD) SDMI Compliant Portable Device;

(PDFM) Portable Device Functional Module;

(PKC) Public Key Cryptosystem;

(PM) Portable Media (SDMI Complaint Storage Media);

($PryKey_A$, $PubKey_A$) Private Key and Public Key of A (A may be LCM, PD, ISP, CA, and the like);

(RMF) Right Management Field;

(RMS-DB) Right Management System-Data Base;

(RNG) Random Number Generation Unit;

(SDMI) Secure Digital Music Initiative;

(SH) Secret Header;

(SNAKE) Symmetric Key Encryption Algorithm, which is very effective for both software and hardware implements and has been world-wide cryptanalized;

(SOI) Source Originator Indicator Field;

(UTD) Update Token Data.

[0047] It should be noted that in the above items the Elliptic Curve based Public Key Cryptosystem is just an example as a candidate of Public Key Cryptosystem, and so any public key cryptosystem, for example RSA, can be used instead of it. But we suggest that SDMI compliant

EMD System (Electronic Music Distributing System) adopt the ECC System for the next generation portable devices, since ECC can be efficiently implemented in such small devices with low cost.

[0048] Also, an internet service provider includes a content provider as well as an information provider via network. A personal computer or an LCM is examples as a candidate of the first content output unit. A portable device such as MP3 is an example of a second content output unit. A portable medium is a general recording medium including smart media.

[0049] FIG. 1 is a schematic view for explaining a system for preventing an illegal copy of digital contents according to an embodiment of the present invention.

[0050] A certificate authority 110 generates a first table having the manufacturer key and the manufacturer key data, and a second table having an identifier (ID) of the portable device 150, a token, T, and the information (ENC(MK_{PD}, T)) of the token encrypted by the manufacturing key. That is, the certificate authority 110 generates the manufacturer key, MK_{PD}, and its certificate data, Cert(MK_{PD}), in accordance with a first registration request signal 121 inputted from a manufacturer 120 of portable devices 150, and outputs a manufacturer key and a manufacturer key data to the manufacturer 120.

[0051] The manufacturer 120 of the portable devices 150 outputs the registration request signal 121 to the certificate authority 110 and receives the manufacturer key and the manufacturer key data generated by certificate authority 110 in accordance with the first registration request signal 121.

[0052] An internet service provider (ISP) 130 including a content provider via the internet outputs a request signal 131 to the certificate authority 110, receives a pair of keys and the certificate of the key which are generated in the certificate authority 110 in response to the registration request signal 131 of the ISP, and the second table from the certificate authority 110.

[0053] A licensed SDMI (secure digital music initiative) compliant module (LCM) 140 as a first content output unit outputs a registration request signal 141 to the internet service provider 130 in order to receive the digital contents, receives the public key and the data of the public key generated in response to the request signal 141, bypasses the data of the manufacturing key of the portable device 150 to the ISP 130, and encodes and outputs the manufacturer key detected from the second table in response to the manufacturer key data.

[0054] The portable device 150 as a second content output unit stores the manufacturer key and the manufacturer key data transferred from the certificate authority 110, outputs its manufacturer key to the internet service provider 130 through the LCM 140, and receives the manufacturer key data of the second table, which is encrypted, supplied from the LCM in order to judge if the stored manufacturer key is authenticated.

[0055] The first table, as shown in FIG. 2, contains the manufacturer key data (Cert(MK_{PD})), the manufacturer key (MK_{PD}), and an identifier (ID_{MK}) corresponding to the manufacturer key data and the manufacturer key, and is stored in only the certificate authority 110. Further, the second table is generated from the certificate authority 110 and outputted to the internet service provider 130, and contains the identifier(ID_{MK}), data (ENC(MK_{PD}, T)), and a token(T) which is encoded by the manufacturing key.

[0056] At this time, the certificate authority 110 forms a first channel key(k) which can be shared with the internet service provider 130 in accordance with the registration request signal 131 inputted from the internet service provider 130, and outputs the first authentication qualification key and the first authentication qualification key data 111 which are encoded into the internet service provider 130 through a secret channel formed by the first channel key(k).

[0057] The first channel key is a key generated from encryption of the certificate authority 110 by using the data which the internet service provider 130 has.

[0058] Here, we present the minimum substances (algorithms) that are needed for the insurance of the security of the LCM and the portable device. It is assumed that the content compressing and decompressing CODECs are built in each device in either software-form or hardware-form.

For the LCM

[0059] Public Key Cryptosystem (PKC), such as ECC, RSA, ... (ECC is more preferable), is to be used for the secure key setup of LCM, the validity check of ISP's Public Key Certificate, and the secure channel construction between ISP and LCM. Symmetric Key Encryption Algorithm, such as SNAKE, is to be used for the content encryption, the authentication to a portable device, and the secure channel construction between LCM and the portable device. How to construct the secure check-in/out and how to securely maintain it are presented in FIGS. 5 and 6.

For the portable device

[0060] Public Key Cryptosystem (PKC) is optional to the portable device 150. Symmetric Key Encryption Algorithm, such as SNAKE, is to be used for the content encryption, the authentication to the LCM, and the secure channel construction between the portable device and the LCM. The manufacturer key, MK_{PD}, which is the pre-set manufacturer key in a temper resistant area within the portable device, is to be used for the secure registration of a portable device to LCM.

For the portable medium

[0061] There needs an apparatus or a pre-set special information within a portable medium to protect contents in it from the dead-copy to another portable medium. It is desirable, we think, to use the unique ID based approach, that is the method that the manufactures of portable media embed a unique ID of each portable medium in the write-protected area of it while they manufacture it. This can be considered as a low-cost method to dead-copy protection for the first generation portable medium.

[0062] Regarding the initiation mechanism of the present invention, there are four registration mechanisms relative to ISPs, LCMs, and PDs. The four registration mechanisms include the registrations of the portable device manufacturers to the certificate authority, of ISP to the certificate authority, of LCM to ISP and of the portable device to LCM, and of multiple LCMs or multiple PDs. The manufactures' registration to the certificate authority precedes all the others.

[0063] The registration of the portable device manufacturer 120 to the certificate authority 110 is illustrated in FIG. 2.

[0064] When the manufacturer 120 requests its registration to the certificate authority 110, the certificate authority 110 certifies it and then generates a manufacturer key, $MK_{PD,}$ and make its certificate data, $Cert_{CA}(MK_{PD})$, to deliver them to the manufacturer 120. At the same time, the certificate authority 110 generates a random token, T, to make (or update) a manufacturer key information table (MKIT) for an ISP-registration. Once after the manufacturer 120 gets the data, $\{MK_{PD}, Cert_{CA}(MK_{PD})\}$, the manufacturer 120 can manufacture the portable devices by imbedding those secrete data within a temper resistant area of the portable devices.

[0065] Therefore, the portable devices 150 manufactured by the manufacturer 120 are authorized by the certificate authority 110 to store the downloaded, encrypted digital contents.

[0066] Fig. 3 shows how for the ISP 130 to register to the certificate authority 110 and what information to get from the certificate authority 110. For the ISP 130 to register to the certificate authority 110, firstly it generates its ephemeral private-public key pair $\{PrvKey_{eph}, PubKey_{eph}\}$ to open a secure channel between the certificate authority and itself by EC_DH(Certificate authority, ISP) and provide a safe way to communicate each other without allowing an illegal copy of the downloaded information through the channel. Secondly, a pair of keys and key data $\{PrvKey_{isp,}$ $PubKey_{isp,}$ $Cert_{CA}(PubKey_{ISP})\}$ are generated and stored in the certificate authority 110, and two tables are formed in dependence with the manufacture key. The certificate authority 110 encrypts and transmits the encrypted key and key data to internet service provider 130 through the channel in order to co-own the key and key data. The ISP 130 gets its semi-permanent private-public key pair $\{PrvKey_{ISP}, Cert_{CA}(PubKey_{ISP})\}$ and the manufacturer key information table data through the security channel. Noting that ISP's key pair should be securely stored, where the host's various system parameters may be used for this goal.

[0067] The LCM registration mechanism to an ISP together with the portable device registration is described. As in Fig. 4, LCM gets the ISP's Public Key Information {$PubKey_{ISP}$, $Cert_{CA}(PubKey_{ISP})$} at first and verifies its validity by using the CA's public key Information which was already announced or preset within the LCM in a code-imbedded-like method. If the validity of the certificate for the ISP's public key is certified, the LCM 140 executes the handshaking protocol to get an ephemeral shared key by utilizing Elliptic Curve based (or other PKC based) Key Exchanging Protocol. Through this secure channel, the ISP can deliver in safe the LCM's permanent private-public key pair for a static secure communication and a secure content transaction between the LCM and the ISP.

[0068] When a request signal 151 is transmitted from the potable device 150 to the LCM 140, the portable device 150 tosses the certificate data for its ID of the manufacturer key to the LCM 140. The LCM 140 sends them to its connected ISP 130 in the encrypted form, EC_ENC($PubKey_{ISP,}$ $Cert_{CA}(ID_{MK})$).

[0069] The internet service provider 130 decrypts the encrypted information and compares the decrypted information with the information of the second table. If the decrypted information is identical to the information of the second table, the internet service provider 130 encrypts the content of the table and transmits it to the LCM 140 in a secure manner. The LCM 140 decrypts the encrypted information to obtain the information of the token. For the LCM 140 and the portable device 140 to set up a shared secret key and to complete the portable device registration, the LCM

140 randomly generates their static and secret channel key, CK_{PD-LCM}, and encrypts and sends $ENC(T,CK_{PD-LCM})||T^*$. Upon receiving these data, the portable device 140 can extract the token value T from T^* by using the manufacturer key and, by using this token, the portable device 140 can also compute CK_{PD-LCM} and store it. As the portable device 140 securely stores this channel key, the portable device registration is finished. The channel key, CK_{PD-LCM}, may be originated from portable device 150 instead of LCM 140. In this case the portable device 150 receives the data T^* from the LCM and gets the token T by decrypting T^* with its manufacturer key. And then the Portable device generates a random channel key CK_{PD-LCM} to upload $ENC(T, CK_{PD-LCM})$ to LCM. The part of the record in the manufacturer key information table (MKIT) of the LCM 140 stays in encrypted form by using the LCM's secret key (this key may be LCM's public key). In practice, during the portable device 150 registration to the LCM 140, an update token data (UTD or update token data) of Right Management System-Data Base (RMS-DB) should be transferred from the portable device 150 to the LCM 140 (or from the LCM 140 to the portable device 150) together with CK_{PD-LCM} and be set both in the RMS-DB and in the portable device. Therefore, all the units and terminals in this system are authorized to transmit and receive the encrypted digital contents between the units and terminals.

[0070] As shown in FIG. 1, the architecture and the file format of the present invention can allow users to register their own limited number of LCMs or PDs. The number may be limited by ISP or by the certificate authority. To register a plurality of LCMs, since ISP maintains the private-public key pair of the firstly registered LCM of a user's multiple LCM's, ISP can securely deliver the same key pair to another LCM of the user. To register a plurality of portable devices, LCM securely maintains the secret channel key between the LCM and the portable device, the LCM can securely deliver the same key pair to another portable device of the user in the same manner depicted in Fig. 4.

[0071] Fig. 5 shows exemplified implementation for the management rule of RMS-DB when a content downloading occurs.

[0072] To manage the information CTC={Copyright, Transfer, Check-in/Check-out}, the LCM 140 maintains the Right Management System Database 143, named RMS-DB in a secure manner. The Right Management System is described, focusing on the content transaction between LCM 140 and the portable device 150.

[0073] The RMS-database contains an update token data area 143a, a title, CTC (copyright, transfer, check-in/check-out) field 143b, a playback control status data area 143c.

[0074] The part of the record in RMS-DB (in LCM) stays in encrypted form by using the LCM's secret key such as CK_{PD-LCM}. The UTD part 143a may have a few number of Updating Token Data depending on the number of a user's own PD's.

[0075] The most important area in the database is the update token area 143a, and the update token area 143a has different values when the update token area 143a downloads a digital content from the LCM 140 to the portable device 150, or uploads the digital content from the portable device 150 to the LCM 140. At this time, the update token is transmitted to the LCM 140 through the portable device 150 to update the stored token in the LCM 140.

[0076] A portable device import control is a layer existing in the LCM 140 to import contents (SDMI Compliant contents from ISPs or non-SDMI Compliant outsource contents (e.g. RedBook CDS, DVD, ...)). Therefore, this layer contains the following three capabilities. One is trans-coding to make the portable device decompress the input with its CODEC. Second is trans-encrypting to make the portable device decrypt the input with its encryption system. Third is to converting the input to SDMI Compliant the format.

[0077] A portable device interface has two capabilities; authenticating to the portable device and opening a secure channel between LCM and the portable device.

[0078] An ISP interface has two capabilities; authenticating to the portable device and opening a secure channel between LCM and the portable device.

[0079] Functional components in the portable device include an LCM interface and an import control within the portable device. The LCM interface has two capabilities; authenticating to LCM and opening a secure channel between the portable device and LCM. The import control within the portable device has the capability to import an outside analog input and to make it fit to the SDMI compliant file format. Where the converted SDMI compliant content should have the binding information to the portable device 150 to be played only via the portable device 150.

[0080] FIG. 6 shows an exemplified file format. As shown in FIG. 6, the SDMI compliant file contains a plain header 610, a secret header 620, and a file body 630. The plain header 610 comprises a title-ID 611, a content description field (CDF) 612, and an algorithm identifying field (AIF) 613.

The secret header 620 contains a device-ID 621, a source originator indicator field (SOI) 622, a copyright holder information field (CHI) 623,a right management field (RMF) 624, and a content encryption key 625. The file body 630 contains a symmetric key encryption of Content by utilizing a secret key (ENC(k, Content)).

[0081] The brief descriptions of the fields are as follows:

--Indication of Source Originator--ISP< LCM (CD-ripping, Audio input)< Portable device (Analog input), Kiosk, ...

--Device identifier--LCM_ID,PD_ID, PM_ID

--Algorithm Identifying Field

--Authentication secret sharing an algorithm identifier--EC (Elliptic Curve)-Signature, EC-DH, ...

--Encryption algorithm identifier

--Codec algorithm identifier--MP3, AAC, ...

--Encryption key information of content

--Right Management Field

Right management field contains the Copy, Check-In/Out, Transfer and Playback Control Status, which are to be encrypted by secret key of the device.

--Copy-Never/Copy-Free/No-More-Copy mode

--Check-In/Out mode

--Transfer mode (Transferable or not)

--Playback control information

--Allowable number of times to be played (unlimited or n-times)

--Expiration date

--Amnesty period

--Copyright holder information

--Content description field--Title, Composer, Artist, Record-label, ...

[0082] The rules to transfer contents securely over ISP-LCM-PD-PM are as follows.

[0083] When the ISP receives a content downloading request from the LCM, it confirms the LCM's ID and then downloads the content with the file format of FIG. 6 to the LCM. For the LCM to play the reached content, it follows the following steps in this order. First, the LCM finds out the encryption algorithm from the AIF 613 in the plain header 610. Second, the fields in the secret header 620 are recovered by using the found out encryption algorithm and LCM's secrete key (private key). Third, the Device-ID field 621 is compared with the ID of the LCM to check if there is correspondence between the two. In the case of correspondence, the copy control status from the RMF data, the playback control status, and the transfer control status are identified to register them in the database(RMS-DB) which the LCM 140 has.

[0084] After the above process is performed, the digital content encryption key is extracted by using a CEK field, and the encoded digital content is interpreted by using the encryption key. If any of these lists is not violated, the music can be played.

[0085] If it is needed to modify the RMF 624, especially the Playback Control Status (PCS), the LCM 140 has to update the data both in the file and in the RMS-DB following the controlling direction.

[0086] In the case of changing the RMF 624 of the file formats, in particular the playback control status, the LCM 140 replaces the playback control state data in two places of the database(RMS-DB) and the file format with desired data.

[0087] The procedure for the LCM 140 to download the content to its portable device 150 includes the following steps. First, the LCM 140 requests the PD-ID and UTD to the portable device 150. Second, the portable device 150 sends the ENC (CK_{PD-LCM}, UTD ll PD-ID) to the LCM 140. Third, the LCM 140 recovers the PD-ID and confirms it. Fourth, the LCM 140 recovers the UTD and the fields in the secret header 620 and compares them with those in its RMS-DB. If UTD is correct and if any alternation of RMF is needed, the LCM updates the contents of RMF both in RMS-DB and in the file format. Fifth, the LCM 140 updates UTD of RMS-DB with newly generated UTD, and ENC ($CK_{PD-LCM, UTD}$*) is to be sent to the Portable device. Sixth, where the Transfer Control Status field has the three types, "Transfer", "Transferred", and "Transfer-non" and the Transfer Control Status in RMS-DB indicates as "Transfer", "Transfer" is replaced with "Transferred" in the Transfer Control Status filed in RMS-DB, but not in the file format. Seventh, if the Copy Control Status (CCS) indicates "Check-in", it is replaced by "Check-out" in the Copy Control Status field both in RMS-DB and in the file format. Eighth, if the Copy Control Status (CCS) indicates "Copy-Never", the content downloading to the portable device is denied. If any of the above lists is not violated, the content to the portable device is downloaded.

[0088] Hereinafter the process of the digital contents between the portable device 150 and the portable recording medium 160 as a content storage medium for preventing an illegal copy in downloading the digital content, which the portable device has, to the portable medium 160 is explained.

[0089] Firstly, if there is its owned ID in the portable medium 160, the portable device 150 records the digital contents which are encrypted by using the ID.

[0090] Secondly, if there is its owned ID in the portable medium 160, the portable device 140 records the digital contents which are encrypted by using randomly generated key.

[0091] The randomly generated key T is encrypted by using a key, S, of the general secret key which is predetermined by the manufacturer 120 of the portable device 150.

[0092] The encrypted T is recorded on the hidden area of the portable medium 160.

[0093] Where there is its own ID in the portable medium 160, all contents within the portable medium can be played by all the portable devices, but, where there is not its own ID, all contents within the portable medium 160 can be played only by the portable devices produced by the manufacturers which adopted this system. Anyway it is certain that this system can support the portability of contents via the portable media.

[0094] As previously we defined, the "Transferability" is a different concept from the "Portability" of a content. The main difference is that the content with "Transferability" can be not only played in any portable devices but also uploaded to any LCMs, but not in the case of "Portability". Since the present system has and manages the Transfer Control Status field both in the RMS-DB and in the file format, the present system can support the transferability of the content. If there is marked "Transfer" in the field of a content and if the content is just downloaded to the portable device, then the LCM downloads it to the portable device and replaces "Transfer" by "Transferred" in the relevant field of RMS-DB. Then the content, which has been downloaded to the portable device, can no longer be played in the LCM until it is uploaded to the LCM again, but the downloaded content in the portable medium 160 can be played by any portable device and can be uploaded to another LCM via the portable device. If the Copy Control Status (CCS) of a content contained in a portable medium indicates "Copy-Free", the content can be uploaded to any LCMs.

[0095] Further, various input devices are additionally connected to the LCM 140 and the portable device 150 applied to the present invention, and such input devices are shown in detail in FIG. 7.

[0096] The input devices which can be additionally connected to the LCM 140 and the portable device 150 can be CD such as RedBook CD, audio CD, super audio CD, DVD Disk, and analog input, and the like.

[0097] The audio signal inputted through the input devices is inputted to the LCM 140, and encoded according to a system supported in the present invention, and then transmitted to the portable device 150, or transmitted to the portable medium 160 to be reproduced through the portable device 150.

[0098] The kiosk 170 generates a registration request signal for selling an encoded digital content by the internet service provider 130 through the LCM 140. Therefore, the internet service provider 130 provides to the kiosk 170 the portable medium 160 having digital contents encoded by the system supported in the present invention according to the registration request signal, and the kiosk receives fees from users and transmits the digital contents stored in the portable medium 160. Kiosk 170 is a store or vending machine selling a recording medium or digital content which is reproduced in this system. Machine on Kiosk is regarded as a personal computer having an interface of the digital content portable medium 160. The recording medium interface can be used by anyone having a supply agreement with an intellectual property right owner or the digital internet service provider.

[0099] FIG. 8 is a view for showing an output source of Fig. 7 capable of being additionally connected to the embodiment of the present invention.

[0100] As shown in Fig 8, the LCM 140, in which the LCM module exists, has at least the following three layers (two of these exist in the LCM module):

[0101] Authenticated Input API 810 has the roles of confirming the validity of the input and extracting some required information to convert the input into a SEMI Compliant format. With respect to the role of confirming the validity of the input, if the input data have a watermark, then this API should be able to detect it. If the input data take an encrypted (or scrambled) form, then this API should be able to extract its encryption key and the encryption (or scrambling) algorithm. If the input data do not take any protected form, then the API should confirm the validity of written format of the media containing the input data. The API checks if an input device and data inputted from the input device are suitable for the system and transmits the following data to the import control layer

820.

[0102] The required data for the API to pass over to the Import Control Layer are as follows:

--Information of the media (source) type--Audio CD, DVD Audio, ...

--Information of the originator of the input content

--Information of the content--Title, if any, Player, Artist, ...

--Information of the encryption algorithm if any

--Information of the encryption key if any.

[0103] The Import Control Layer 820 gets a bundle of information from the Authenticated Input API and reconstructs the input content to meet a SEMI Compliant file format by following the rules listed below:

--Copy Control Status--mark "Copy-Never" or "Check-in/Check-out" (optionally)

--Playback Control Status--mark "Times to playback = infinite or N" (N: optional)

--Transfer Control Status--mark "Transfer-Non"

--Mark the "LCM-ID" into the SOI field and Device-ID field of SH (Secret Header)

--If the input content is not encrypted, a random key is generated and encrypts the input content by the random key.

--If the input content takes an encrypted form by other encryption algorithm different from the PD's, then this layer trans-encrypts the content to be played in the portable device.

--The secret header part is encrypted by LCM's public key.

[0104] The PD Interface layer 830 authenticates the connected portable device 150 by checking whether the portable device 150 has its correct ID and the secret channel key, CK_{PD-LCM}. The Kerberos Authentication Protocol may be used (refer to: A.J. Menezes, P.C. Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, pp. 401-403, CRC Press, 1996).

[0105] The Import Control Layer (ICL) 860 within the portable device 150 makes a SEMI Compliant compressed digital content from the analog input by following the rules listed below:

--Upon reception of each frame of the analog input, the ICL encodes the frame and by a randomly generated key. If all the frames have been encrypted, the next steps are followed.

–The copy control status is marked as "Copy-Never" or "Check-in/Check-out" (optionally).

–The playback control status is marked as "Times to playback--infinite or N" (N: optional).

–The transfer control status is marked as "Transfer-Non".

–The "PD-ID" is marked into the SOI field and Devide-ID field of the secret header,

–The portable device encrypts the secret header part by the portable device's channel key.

[0106] If the converted SEMI Compliant content from the analog input has its SOI field 622 of the Secret Header with marked "PD-ID", then the procedure of writing the content on a portable medium does not use the unique ID of the portable medium. This means that such content as made from an analog input to a portable device is not allowed to have the "Portability".

[0107] Hereinafter, the copy protection scheme for portable media is described.

[0108] The portable medium may optionally support unique ID for first Generation portable media. If the unique ID is not supported, the physical address of a bad sector of the portable medium is used instead. If unique ID is supported, it should be one-time writeable during the manufacturing stage only, and readable only by the portable device with a special command.

[0109] The copy protection system for the portable media is shown in FIG. 9.

[0110] First, the portable device 150 and the LCM 140 share a channel key to form a secure channel between them.

[0111] The portable device 150 receives as inputs and function processes a physical address of a bad sector of the portable medium 160, a random number, and a secret channel key which is transmitted from the LCM 140 and stored in the LCM 140. With the processed value, the portable device 150 encrypts a header of the digital contents and transmits it 160. Hash function or one way function can be used for the function process. At this time, what generates the key for encryption is the function process means 149.

[0112] Function process means 149 receives as an input the physical address of the bad sector transmitted from the portable medium 160 and receives as an input the random number through the random number generating means (RNG) 159. The random number is also transmitted and stored in a spare area of the portable medium 160.

[0113] The portable medium 160 transmits the physical address of the bad sector, stores a random number generated in the portable device 150 as an input in the spare area, and stores as sector data the encrypted header information encrypted by the processed value and the encrypted digital content inputted through the portable device 150.

[0114] It is optional to encrypt the header of the digital content by function processing after receiving all of the commonly owned key, random number, and the physical address of the bad sector or one of the commonly owned key, random number, and the physical address of the bad sector.

[0115] The digital content can be downloaded to the portable medium 160 through the portable device 150 or directly from the LCM 140.

[0116] Even if the portable medium is copied to another portable medium, the digital content in the portable medium cannot be reproduced from the portable medium. Therefore, this invention provides the effect on basically protecting illegal copy.

[0117] As stated above, the preferred embodiments of the present invention are shown and described. Although the preferred embodiments of the present invention have been described, it is understood that the present invention should not be limited to these preferred embodiments but various changes and modifications can be made by one skilled in the art within the spirit and scope of the present invention as hereinafter claimed.